

Tribunal da Relação de Lisboa
Processo nº 103/21.8TELSB-A.L1-5

Relator: SANDRA OLIVEIRA PINTO

Sessão: 25 Outubro 2022

Número: RL

Votação: UNANIMIDADE

Meio Processual: RECURSO PENAL

Decisão: NÃO PROVIDO

LEI DO CIBERCRIME

APREENSÃO DE CORREIO ELETRÓNICO

AUTORIZAÇÃO

DESPACHO JUDICIAL PRÉVIO

NULIDADE

Sumário

I - Face à arquitetura normativa patente na Lei do Cibercrime, tem de entender-se que o regime previsto no artigo 16º deve aplicar-se sempre que esteja em causa a apreensão de dados informáticos e o do artigo 17º sempre que esteja em causa a apreensão de correio eletrónico e registo de comunicações de natureza semelhante – que, sendo dados informáticos em si mesmos, se apresentam como qualitativamente diversos, em função do nível de intromissão na vida privada e nas comunicações que a sua apreensão é suscetível de importar.

II - A apreensão de correio eletrónico ou de registos de comunicações de natureza semelhante carece, sob pena de nulidade, de despacho judicial prévio.

III - Se, ao determinar a realização de busca não domiciliária, o MP antevê a apreensão de mensagens de correio eletrónico, tem de solicitar – e obter – previamente autorização judicial para o efeito, não podendo determinar a apreensão de «dados eletrónicos» para posterior apresentação ao Juiz de Instrução para validação.

IV - Estando o MP ciente, ao determinar a realização da busca não domiciliária, de que a mesma teria como consequência a interferência em dados protegidos – nomeadamente, comunicações de correio eletrónico – não pode acolher-se àquela que se configura como válvula de segurança do

sistema, a situação excecional tida em vista no artigo 16º da Lei do Cibercrime. Aceitar tal asserção seria sufragar, precisamente, a posição que o acórdão TC 678/2021 julgou inconstitucional.

(sumariado e confidencializado pela relatora)

Texto Integral

Acordam, em conferência, na 5ª Secção do Tribunal da Relação de Lisboa:

I. Relatório

No processo nº 103/21.8TELSB, a correr termos no Departamento de Investigação e Ação Penal de Lisboa, foi proferido, em 27.05.2022, pelo Juiz 7 do Tribunal Central de Instrução Criminal, despacho que, “ao abrigo do disposto nos arts. 17.º da Lei n.º 109/2009, de 15 de Setembro, e 179.º do Código de Processo Penal declaro[u] nula a apreensão da correspondência que consta da *pen drive* do saco de prova Série A com o nº 130076, não podendo, por isso, o tribunal tomar conhecimento da mesma”.

*

Inconformado com tal decisão, dela interpôs recurso o Ministério Público, extraído da respetiva motivação as seguintes conclusões:

“1. A Mma. Juiz a quo declarou, no despacho de que ora se recorre, a nulidade de um acto - de ordenar a apreensão de correspondência electrónica - que o Ministério Público não praticou, confundindo a apreensão de dados electrónicos, efectivamente, por si determinada, com a apreensão de correspondência que, casualmente, se verificou estar contida em determinados equipamentos e que - selada - lhe foi, para o efeito, apresentada.

2. Justificou essa sua decisão com a necessidade de uma prévia autorização judicial que, não obstante, à cautela, lhe tivesse sido, antecipada e expressamente, promovida, optou por não conceder ou, por outro lado, se negar a conceder, silenciando nesse particular.

3. A omissão em causa - caso se deva concluir pela necessidade de tal autorização judicial (prévia) - configura nulidade, por omissão de pronúncia, o que se argui, ao abrigo do preceituado no art.º 379º nº 1 alínea c) do Código de Processo Penal.

4. A nosso ver, porém, a autorização em causa não é sequer necessária porquanto se está perante busca não domiciliária e é ao Ministério Público - que determinou a realização de busca não domiciliária - que incumbe autorizar “a pesquisa informática, com vista à apreensão de documentação

guardada em suporte digital e armazenada em sistemas informáticos ou noutros sistemas aos quais seja possível aceder através destes, incluindo comunicações de correio eletrónico”, conforme entendimento jurisprudencial pacífico.

5. A correspondência em causa foi selada e, prontamente, apresentada à Mma. Juiz de Instrução, com observância estrita do preceituado no art.º 17º da Lei do Cibercrime e, subsidiariamente (por remissão do mesmo), no art.º 179º do Código de Processo Penal.

6. Incumbia-lhe, pois, tomar conhecimento da mesma, em primeira mão, e, caso o entendesse pertinente, determinar a respectiva junção aos autos.

7. Pelo que, não o tendo feito, o douto despacho da Mma. Juiz deve, em nosso entender, ser revogado, substituindo-se por outro que designe data para abertura de correspondência.”

*

O recurso foi admitido, a subir imediatamente, em separado e com efeito suspensivo.

Neste Tribunal, o Exmo. Sr. Procurador-Geral Adjunto emitiu parecer no sentido da procedência do recurso.

Proferido despacho liminar e colhidos os “vistos”, teve lugar a conferência.

*

II - questões a decidir

Como é pacificamente entendido, o âmbito dos recursos é definido pelas conclusões extraídas pelo recorrente da respectiva motivação, que delimitam as questões que o tribunal *ad quem* tem de apreciar, sem prejuízo das que forem de conhecimento oficioso (cf. Germano Marques da Silva, *Curso de Processo Penal*, vol. III, 2ª ed., pág. 335, Simas Santos e Leal-Henriques, *Recursos Penais*, 9ª ed., 2020, págs. 89 e 113-114, e, entre muitos outros, o acórdão do Supremo Tribunal de Justiça de 05.12.2007, Processo nº 3178/07, 3ª Secção, disponível in Sumários do STJ, www.stj.pt, no qual se lê: «*O objecto do recurso é definido e balizado pelas conclusões extraídas da respectiva motivação, ou seja, pelas questões que o recorrente entende sujeitar ao conhecimento do tribunal de recurso aquando da apresentação da impugnação - art.º 412.º, n.º 1, do CPP -, sendo que o tribunal superior, tal qual a 1.ª instância, só pode conhecer das questões que lhe são submetidas a apreciação pelos sujeitos processuais, ressalvada a possibilidade de apreciação das questões de conhecimento oficioso, razão pela qual nas alegações só devem ser abordadas e, por isso, só assumem relevância, no sentido de que só podem ser atendidas e objecto de apreciação e de decisão, as questões suscitadas nas conclusões da motivação de recurso, (...), a significar que todas as questões incluídas nas alegações que extravasem o objecto do recurso terão de ser*

consideradas irrelevantes.»)

Atentas as conclusões apresentadas, que traduzem as razões de divergência do recurso com a decisão impugnada - o despacho que declarou nula a apreensão de correspondência eletrónica - a única questão a examinar e decidir é a de saber se o Ministério Público, sem prévia autorização do Juiz de Instrução, pode determinar a apreensão de correio eletrónico que venha a ser encontrado em pesquisa informática por si determinada, para posterior validação pelo Juiz de Instrução.

*

III - Decisão Recorrida

É do seguinte teor o despacho recorrido (transcrição):

“A pen drive do saco de prova Série A com o nº 130076 refere-se à correspondência electrónica cuja apreensão não foi autorizada judicialmente. Nos presentes autos o Ministério Público determinou a realização de busca a um escritório de contabilidade, decidindo a apreensão de correspondência electrónica e outros dados dos suspeitos.

Nessa sequência apresentou a correspondência electrónica apreendida para conhecimento judicial, para exame e decisão da sua junção aos autos, nos termos dos artigos 179.º do Código de Processo Penal e 17.º da Lei n.º 109/2009, de 15 de Setembro.

No entanto, não se compreende a validade desta apreensão de correspondência, particularmente com referência às mencionadas disposições legais.

No caso específico da correspondência (art.º 179.º do Código de Processo Penal), estabelece a Lei que essa apreensão deve ser autorizada ou ordenada pelo juiz, verificados os demais pressupostos estabelecidos no art.º 179.º, n.º 1, do Código de Processo Penal (pressupostos que aqui não se discutem).

Nessa circunstância, o juiz é o primeiro a tomar conhecimento de tal apreensão que ordenou, de forma a apreciar da validade do que foi apreendido e, após a indicação pela investigação do que mostrar necessário, decidir sobre a sua junção aos autos (art.º 179.º, n.º 3, do Código de Processo Penal).

Não se percebe como pôde o Ministério Público autorizar expressamente a apreensão de correspondência sem autorização judicial (neste local), particularmente com a invocação do preceito referido e, sobretudo, querendo executar apenas a parte final do mencionado mecanismo processual de garantia.

Em particular quanto à apreensão de correspondência electrónica, cabe ao tribunal autorizar ou ordenar a sua apreensão, de acordo com o disposto no art.º 17.º da Lei n.º 109/2009, de 15 de Setembro, que, na sua parte final, remete para a mesma regulamentação processual penal (cfr. o teor do Acórdão

do TC n.º 687/2021).

Essa disposição da Lei do Cibercrime apenas permite, de forma específica, a possibilidade de, no decurso de uma pesquisa legitimamente autorizada, ser encontrada por acaso correspondência electrónica (uma vez que, sendo desconhecida a correspondência, não era possível obter a prévia autorização para a sua apreensão).

Nessa situação, os dados de correspondência são isolados e apresentados judicialmente.

Mas não é essa a situação que se apresenta nos autos.

Aqui foi o Ministério Público que determinou a realização de uma busca, ali incluindo expressamente a pesquisa por correspondência e a sua apreensão. Nesse tipo de situação em que, previamente à realização de uma diligência, o Ministério Público pretende a apreensão de correspondência de qualquer tipo, terá a mesma de ser autorizada judicialmente, por forma a que seja controlado previamente o próprio acesso a tais dados ou elementos físicos, de acordo com a previsão do art.º 179.º do Código de Processo Penal, ali se incluindo a proporcionalidade e a necessidade do determinado (como ocorreu quanto à busca à residência autorizada).

E tal é coerente com a exigência de autorização judicial na medida do necessário à obtenção de conteúdos de comunicação, mesmo já consumados, e não apenas à sua interceptação (arts. 187.º e 189.º do Código de Processo Penal).

A referida autorização judicial é exigida sob pena de nulidade (art.º 179.º, n.º 1, do Código de Processo Penal) e não se verificou neste caso.

Por isso, ao abrigo do disposto nos arts. 17.º da Lei n.º 109/2009, de 15 de Setembro, e 179.º do Código de Processo Penal declaro nula a apreensão da correspondência que consta da pen drive do saco de prova Série A com o nº 130076, não podendo, por isso, o tribunal tomar conhecimento da mesma.”

*

Em 04.05.2022, o titular do inquérito proferiu o seguinte despacho (transcrição parcial):

“3. Busca Domiciliária

Reproduzindo a factualidade supra descrita e o seu enquadramento, sustentados pelos elementos probatórios já recolhidos no âmbito deste inquérito, é seguro afirmar que existem já indícios suficientes de que a sociedade A..., Lda., estará a ser instrumentalizada - por um grupo de indivíduos, deles já estando identificados os suspeitos A...R..., na qualidade de gerente da referida sociedade, e J... L..., enquanto beneficiário efectivo - para a comissão de crime de branqueamento de capitais, previsto e punido pelo art. 368.º-A, n.ºs 1 e 2 do Código Penal.

Com vista ao apuramento cabal da descrita actuação dos suspeitos, e com vista a proceder à identificação de quem consigo mais actua e bem ainda com o propósito de recolher e detalhadamente analisar a documentação contabilística que exista com referência às transações realizadas pela sociedade A..., Lda., justificativas, ou não, dos muito avultados fluxos financeiros que movimenta, o que, reflexamente, permitirá também apurar eventuais valores de impostos que a sociedade visada teria de ter liquidado e que não terá pago, surge como indispensável para a integral descoberta da verdade material e da extensão da actividade delituosa sob investigação o recurso a meios de obtenção de prova que colidem com direitos fundamentais, designadamente, o direito à reserva da intimidade da vida privada e a inviolabilidade do domicílio, nos termos previstos pelo art.º 32º n.º 8 e art.º 34º n.º 2 e 3 da Constituição da República Portuguesa, uma vez que a sede da sociedade A..., Lda., situada na Rua ..., em Lisboa, é simultaneamente o domicilio pessoal de R... P..., sua colaboradora/funcionária.

É, deste modo, imprescindível para o avanço da investigação em curso, mormente com vista à obtenção de elementos de prova que confirmem as sustentadas suspeitas que sobre os suspeitos recaem da prática de crime de branqueamento de capitais, a realização de busca domiciliária à sua sede da sociedade visada, simultaneamente residência da sua colaboradora R... P..., pois é de crer que ali se encontre arquivada documentação relacionada com a prática dos factos supra descritos.

Nesta conformidade:

- Por ser indispensável para a investigação em curso, mormente com vista à recolha e apreensão de documentação, contabilística, financeira ou de outra espécie, quer enquanto meio, quer enquanto resultado, da comissão do aludido crime de branqueamento de capitais e até mesmo dos crimes precedentes, com que a sociedade comercial *supra* aludida e A... R..., na qualidade de seu gerente, J... L..., enquanto beneficiário efectivo, e a própria colaboradora da sociedade, R... P..., e bem ainda terceiros, se encontram comprometidos, promovo seja determinada busca e ordenada a passagem dos respectivos mandados, nos termos dos arts. 174º, n.º 2 e 3, 177º, n.º 1, 178º n.º 3 e 269 n.º 1 al. c) todos do Código Processo Penal, a cumprir pela Polícia Judiciária no prazo de 30 dias, à residência e anexos dependentes, arrecadações, sótãos, garagens, armazéns e viaturas que se encontrem no seu interior de:

R... P... simultaneamente sede social da sociedade A..., Lda., - sita:

. na Rua ..., em Lisboa.

*

4. Buscas não domiciliárias.

Tendo por fundamento o já supra exposto e para os efeitos igualmente supra indicados, considerando que a sociedade T..., Lda. é o gabinete de contabilidade que trata da contabilidade da sociedade suspeita A..., Lda., de harmonia com o preceituado nas disposições conjugadas dos artigos 34º nº2 da Constituição da República Portuguesa, 174º, n.ºs 2 e 3, 176º, 178º, todos do Código de Processo Penal, determino a realização de busca à sede da seguinte sociedade e gabinete de contabilidade:

- T..., Lda., - sita:
. na Av. ..., Loures;
*

5. Apreensão de dados informáticos

De harmonia com o preceituado nos arts. 11º alínea c), 15º e 16º da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime) desde já autorizo a PJ a, aquando da realização das buscas domiciliárias e não domiciliárias, efectuar a pesquisa e apreensão de dados informáticos nos equipamentos informáticos que se encontrem nos locais das buscas ou acessíveis remotamente a partir desses mesmos locais, ainda que armazenados em eventuais drives/sistemas virtuais de *cloud* ou similares, sempre com a ressalva do preceituado no art.º 17º nº1 da Lei do Cibercrime, devendo o OPC, caso encontre correio electrónico ou registos de comunicações de natureza semelhante, mantê-los fechados, de modo a que seja o Mmo. JIC, nos termos previstos pelo art.º 179º nº3 do Código de Processo Penal, a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, com vista a que, caso se considere relevante para a prova, venha a mesma a ser oportunamente junta aos autos.
*

6. Apreensão de Correio Electrónico e registo de comunicações de semelhante natureza

Caso, na sequência da pesquisa e apreensão de dados autorizada em 5 supra, o OPC, venha, no decurso da mesma, a localizar correio electrónico ou registos de comunicações de natureza semelhante, desde já mais promovo que o Mmo. JIC autorize a apreensão através de cópia/clonagem das referidas mensagens de correio electrónico ou registos de comunicações de natureza semelhante, designadamente os realizados através das aplicações móveis Whatsapp, Skype, Viber, Messenger, Facebook, e ou similares, que se encontrem armazenadas em computadores, telemóveis ou noutros suportes e estejam relacionadas com a factualidade sob investigação nos presentes autos, revelem ser relevantes para a descoberta da verdade material e ou possam constituir prova da prática dos factos aqui integrantes da comissão dos crimes investigados, tudo de harmonia com o preceituado nos arts. 11º alínea c), 15º e 17º da Lei nº 109/2009, de 15 de Setembro e do art.º 179º nº3 do Código de

Processo Penal.”

*

Nessa sequência, foi proferido pela Mma. Juiz de Instrução, em 05.05.2022, despacho com o seguinte teor (transcrição parcial):

“III. Mandados de busca

Investiga-se nestes autos a prática do crime de branqueamento de capitais, previsto e punido pelo art.º 368.º-A, n.ºs 1 e 2, do Código Penal.

Nesta investigação existem já indícios suficientes de que a sociedade A..., Lda., estará a ser instrumentalizada por um grupo de indivíduos com vista à concretização do branqueamento de vantagens obtidas com a prática de crimes.

Os factos em investigação causam alarme e perturbação na vida em sociedade, concretamente devido à repetição criminosa e à dificuldade da sua investigação.

De acordo elementos de prova recolhidos, tal como refere a PJ, há razões para crer que a requerida busca se reveste de grande interesse para a descoberta da verdade e para a aquisição de meios de prova - designadamente apreensão de objectos/documentos/dados informáticos, relacionados com o crime em investigação acima referido - sendo proporcionais a restrição do direito da reserva da vida privada dos visados precisamente em função dos indícios já recolhidos no processo e da sua necessidade para a investigação (arts. 18.º e 34.º da CRP).

A pesquisa e apreensão de dados e correspondência em equipamentos dos visados ou utilizados pelos mesmos ou por alguém segundo as suas indicações, nas residências ou locais a seguir mencionadas e/ou com as pessoas encontradas nos referidos locais, incluindo quaisquer equipamentos informáticos e telemóveis (designadamente com memórias e cartões SIM), bem como a revista das pessoas e viaturas ali encontradas ou pertencentes ou utilizadas pelos mencionados suspeitos ou arguidos nestes autos, podem ser efectuadas, pelos mesmos fundamentos, sendo as pesquisas e apreensão de dados informáticos efectuadas nos termos definidos na Lei n.º 109/2009, de 15 de Setembro, designadamente nos seus arts. 15.º a 18.º, ou seja, ainda que os mesmos respeitem a comunicações, dados referentes à vida privada ou a qualquer tipo de sigilo, desde que, neste caso, seguidamente seja respeitado o procedimento legalmente devido quanto à apresentação judicial desses dados (apenas quanto aos dados sigilosos ou de reserva da vida privada), especificamente por aplicação do estabelecido nos arts. 15.º a 18.º da Lei n.º 109/2009, com a aplicação correspondente dos arts. 179.º a 183.º e 187.º a 189.º do Código de Processo Penal (destacando-se a aplicação do disposto no art.º 179.º, n.º 3, do Código de Processo Penal, quanto à apreensão de correio

electrónico por remissão do disposto no art.º 17.º da Lei n.º 109/2009, de 15 de Setembro).

Assim, por estarem reunidos os pressupostos legais – arts. 174.º, nºs 2 e 3, 176.º e 177.º do Código de Processo Penal – autorizo a realização da busca requerida no seguinte local, possíveis anexos, garagens e arrecadações, com recurso, aos meios coercivos necessários:

Residência sita na Rua ..., em Lisboa.

Passe os competentes mandados, os quais deverão ser acompanhados de cópia deste despacho.

A realização desta busca ficará a cargo da PJ e consigno que não presidirei à mesma.

Prazo: 30 dias a contar deste despacho.

D.N.”

Sobre o ponto 6. da promoção do Ministério Público, por reporte à busca não domiciliária por este determinada, a M^{ma} Juiz de Instrução nada consignou no despacho proferido em 05.05.2022, nada mais lhe tendo sido requerido, posteriormente, quanto a tal questão.

*

Em 18.05.2022, no cumprimento do Mandado de Busca e Apreensão emitido em 12.05.2022 (ref^a *Citius* 415751029), a Polícia Judiciária realizou uma busca nas instalações de “T..., Ld^a”, tendo, entre o mais, procedido à apreensão de: “Doc. 1: Correspondência electrónica, vulgo *e-mail’s*, mantida entre o escritório de contabilidade, melhor identificado em epígrafe – através do endereço de correio electrónico clientes@...pt – e a sociedade A..., Ld^a (NIPC ...), bem como as suas designações sociais anteriores, mormente W..., Ld^a e K..., Ld^a, acondicionada numa (1) *pendrive* da marca «Intenso».” (ref^a *Citius* 7919672).

*

IV – Fundamentação

Como acima se assinalou a única questão trazida a este Tribunal de Recurso é a de saber se o Ministério Público, sem prévia autorização do Juiz de Instrução, pode determinar a apreensão de correio eletrónico que venha a ser encontrado em pesquisa informática por si determinada, para posterior validação pelo Juiz de Instrução.

À matéria em apreciação é aplicável a Lei nº 109/2009, de 15 de setembro (Lei do Cibercrime), atenta a previsão do respetivo artigo 11º, nº 1 [em especial a alínea *c*)], e considerado o objeto da decisão de apreensão (cf. artigo 2º, alíneas *a*) e *b*) do citado diploma legal).

Vejam, então, as disposições legais pertinentes.

Nos termos do artigo 15º, nº 1, da Lei do Cibercrime: “Quando no decurso do

processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência”.

Por seu turno, sobre a «apreensão de dados informáticos», dispõe o artigo 16º, do citado diploma, que: “1. Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.

2. O órgão de polícia criminal pode efetuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

3. Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto. (...)”.

Por fim, sob a epígrafe «apreensão de correio eletrónico e registos de comunicações de natureza semelhante», prescreve o artigo 17º: “Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutra a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurarem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.”

Como, com inegável relevância, se considerou no Acórdão do Tribunal

Constitucional nº 687/2021^[1], “As normas *sub judice* permitem a ingerência na correspondência eletrónica, podendo também, como se procurou mostrar, possibilitar o conhecimento de uma série de dados pessoais que, mesmo que não se entendam respeitantes a um processo de comunicação em curso, sempre serão protegidos pelo direito fundamental à proteção de dados no domínio da utilização da informática, previstos no artigo 35.º, n.ºs 1 e 4, da CRP, enquanto dimensão específica da reserva de intimidade da vida privada, tutelada pelo artigo 26.º, n.º 1, da Lei Fundamental.

Na verdade, as operações necessárias à apreensão de correio eletrónico ou de mensagens de natureza semelhante no decurso de uma pesquisa a um sistema informático importam um risco considerável - senão mesmo a inevitabilidade - de acesso a dados pessoais protegidos, relativos à correspondência do utilizador, bem como a dados de tráfego e de conteúdo abrangidos pela garantia constitucional de inviolabilidade do sigilo. Na generalidade dos casos, é, pois, dificilmente evitável que, no decurso da pesquisa a um computador, o investigador depare com o elenco das últimas mensagens de correio eletrónico e de natureza similar recebidas, identificadas a partir de elementos - como o remetente, o assunto e a data de receção - que estão inequivocamente compreendidos no âmbito da garantia constitucional do sigilo na correspondência. Em algumas situações, pode mesmo ocorrer que o conteúdo da mensagem se esgote, literal ou substancialmente, na identificação do respetivo assunto, pelo que os dados acessíveis incluirão *todos* os dados de conteúdo relevantes.”

Para o efeito que aqui nos ocupa, importa ter presente que a Lei nº 109/2009, de 15 de setembro, transpôs para a ordem jurídica interna a Decisão Quadro nº 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adaptou o direito interno à Convenção sobre Cibercrime do Conselho da Europa, adotada em Budapeste em 23 de novembro de 2001 (aprovada pela Resolução da Assembleia da República nº 88/2009, de 10 de julho de 2009, e ratificada pelo Decreto nº 91/2009, de 15 de setembro^[2]), constando especialmente deste último instrumento, no respetivo artigo 15º, sob a epígrafe «condições e garantias», que *“1 - Cada Parte deverá assegurar que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos na presente secção respeitem as condições e garantias previstas no seu direito interno, o qual deverá garantir uma proteção adequada dos direitos humanos e das liberdades, designadamente dos direitos estabelecidos em conformidade com as obrigações assumidas pela Parte em virtude da Convenção do Conselho da Europa de 1950 para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e do Pacto Internacional sobre os Direitos Cívicos e Políticos das Nações Unidas de 1966, bem como de outros instrumentos internacionais aplicáveis em matéria de direitos humanos, e deverá incorporar o princípio da proporcionalidade.*

2 - Sempre que tal se justifique, em razão da natureza do poder ou do procedimento em causa, as referidas condições e garantias deverão incluir, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a delimitação do âmbito de aplicação e a duração do poder ou procedimento em

causa. (...)”

As opções do legislador nacional, nesta matéria, têm, pois, de ser analisadas no quadro do direito da União, tal como tem sido interpretado pelo Tribunal da Justiça da União Europeia (TJUE), cabendo destacar, como dá conta o Tribunal Constitucional no citado acórdão nº 687/2021, que “em primeiro lugar, resulta evidente que a CDFUE^[3] não é compatível com práticas de recolha e conservação de dados de ordem *indiferenciada e generalizada*, sem uma qualquer *seleção prévia*, segundo *critérios objetivos*. Ora, isto deve levar-nos a questionar se, na generalidade dos casos, é compatível com o direito da União a apreensão de *todas* as mensagens de correio eletrónico (que poderão, mesmo no caso de computadores de uso estritamente pessoal, atingir números na casa dos largos milhares), devendo a seleção do conjunto de mensagens apreendidas limitar-se *ao estritamente necessário* para investigação e repressão da criminalidade. Em segundo lugar, e com evidente importância no presente processo, resulta da jurisprudência exposta que o acesso pelas autoridades nacionais a dados de comunicação, ainda que para combate à criminalidade, deverá ser sempre sujeito a *controlo judicial* ou de *entidade administrativa independente* – ideia que veio a ser retomada no recente acórdão de 2 de março de 2021, Processo C-746/18, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*, adiante analisado, o qual se debruça, justamente, sobre a questão de saber que entidades, ao certo, podem figurar neste papel de *controlo prévio*, designadamente saber se o Ministério Público pode desempenhar tal tarefa.” No mencionado acórdão de 02.03.2021, Processo C-746/18, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*^[4], o TJUE enfrentou diretamente a questão de saber se a uma entidade como o Ministério Público, cuja missão é dirigir a instrução penal e exercer, sendo caso disso, a ação pública num processo posterior, pode ser atribuída competência para autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal.

E, expressivamente, consignou, nos n.ºs 49 a 59, que “Em especial, uma regulamentação nacional que regula o acesso das autoridades competentes a dados de tráfego e a dados de localização conservados, adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, não se pode limitar a exigir que o acesso das autoridades aos dados responda à finalidade prosseguida por essa regulamentação, mas deve igualmente prever as condições materiais e processuais que regem essa utilização (Acórdãos de 6 de outubro de 2020, *Privacy International*, C-623/17, EU:C:2020:790, n.º 77, e de 6 de outubro de 2020, *La Quadrature du Net e o.*, C-511/18, C-512/18 e C-520/18,

EU:C:2020:791, n.º 176 e jurisprudência referida). (49)

Assim, e uma vez que um acesso geral a todos os dados conservados, independentemente de qualquer ligação, no mínimo indireta, com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário, a regulamentação nacional em causa deve basear-se em critérios objetivos para definir as circunstâncias e as condições em que o acesso aos dados em causa deve ser concedido às autoridades nacionais competentes. A este respeito, tal acesso só poderá, em princípio, ser concedido, em relação com o objetivo de luta contra a criminalidade, aos dados de pessoas que se suspeita estarem a planejar, irem cometer ou terem cometido uma infração grave ou, ainda, estarem envolvidas de uma maneira ou de outra nessa infração. Todavia, em situações especiais, como aquelas em que os interesses vitais da segurança nacional, da defesa ou da segurança pública sejam ameaçados por atividades terroristas, o acesso aos dados de outras pessoas poderia igualmente ser concedido quando existam elementos objetivos que permitam considerar que esses dados poderiam, num caso concreto, contribuir efetivamente para a luta contra essas atividades (v., neste sentido, Acórdãos de 21 de dezembro de 2016, *Tele2*, C-203/15 e C-698/15, EU:C:2016:970, n.º 119, e de 6 de outubro de 2020, *La Quadrature du Net e o.*, C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 188). (50)

A fim de garantir, na prática, o pleno respeito destes requisitos, é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja, em princípio, sujeito a uma fiscalização prévia efetuada por um órgão jurisdicional ou por uma entidade administrativa independente e que a decisão desse órgão jurisdicional ou dessa entidade seja tomada na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de perseguição penal. Em caso de urgência devidamente justificada, a fiscalização deve ser efetuada em prazos curtos (v., neste sentido, Acórdão de 6 de outubro de 2020, *La Quadrature du Net e o.*, C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.º 189 e jurisprudência referida). (51)

Essa fiscalização prévia exige, designadamente, como salientou, em substância, o advogado-geral no n.º 105 das suas conclusões, que o órgão jurisdicional ou a entidade encarregada de efetuar a referida fiscalização prévia disponha de todas as atribuições e apresente todas as garantias necessárias com vista a assegurar uma conciliação dos diferentes interesses e direitos em causa. Quanto, mais especificamente, a um inquérito penal, tal fiscalização exige que esse órgão jurisdicional ou essa entidade possa assegurar um justo equilíbrio entre, por um lado, os interesses ligados às necessidades do inquérito no âmbito da luta contra a criminalidade e, por

outro, os direitos fundamentais ao respeito da vida privada e à proteção dos dados pessoais das pessoas às quais o acesso diz respeito. (52)

(...)

A circunstância de o Ministério Público ser obrigado, em conformidade com as regras que regulam as suas competências e o seu estatuto, a verificar os elementos incriminatórios e ilibatórios, a garantir a legalidade da instrução do processo e a agir unicamente nos termos da lei e segundo a sua convicção não basta para lhe conferir o estatuto de terceiro em relação aos interesses em causa na aceção descrita no n.º 52 do presente acórdão. (56)

Daqui resulta que o Ministério Público não está em condições de efetuar a fiscalização prévia referida no n.º 51 do presente acórdão. (57)

Tendo o órgão jurisdicional de reenvio suscitado, por outro lado, a questão de saber se a falta de fiscalização efetuada por uma autoridade independente pode ser suprida por uma fiscalização posterior, exercida por um órgão jurisdicional, da legalidade do acesso de uma autoridade nacional aos dados de tráfego e aos dados de localização, importa salientar que a fiscalização independente deve ser efetuada, como exige a jurisprudência recordada no n.º 51 do presente acórdão, previamente a qualquer acesso, salvo em caso de urgência devidamente justificada, devendo, nesse caso, a fiscalização ser efetuada em prazos curtos. Como salientou o advogado-geral no n.º 128 das suas conclusões, essa fiscalização posterior não permitiria responder ao objetivo de uma fiscalização prévia, que consiste em impedir que seja autorizado um acesso aos dados em causa que ultrapasse os limites do estritamente necessário. (58)

Nestas condições, há que responder à terceira questão prejudicial que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que atribui competência ao Ministério Público, cuja missão é dirigir a instrução do processo penal e exercer, sendo caso disso, a ação pública num processo posterior, para autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal. (59)” (sublinhados nossos)

É, pois, neste quadro interpretativo que têm de ser encaradas as disposições legais que acima se deixaram transcritas, mantendo presente que, nos termos previstos no artigo 269º, nº 1, alínea d) do Código de Processo Penal “*durante o inquérito compete exclusivamente ao juiz de instrução ordenar ou autorizar: (...) d) Apreensões de correspondência, nos termos do nº 1 do artigo 179º*”.

Por seu turno, o citado artigo 179º do Código de Processo Penal (sob a epígrafe *Apreensão de correspondência*) dispõe que: “1- *Sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas*

estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, quando tiver fundadas razões para crer que: a) A correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa; b) Está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos; e c) A diligência se revelará de grande interesse para a descoberta da verdade ou para a prova. (...)

3- O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito, não podendo ser ela utilizada como meio de prova, e fica ligado por dever de segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova”.

Pode, pois, afirmar-se, face à arquitetura normativa patente na Lei do Cibercrime que o regime previsto no artigo 16º deve aplicar-se sempre que esteja em causa a apreensão de dados informáticos e o do artigo 17º sempre que esteja em causa a apreensão de correio eletrónico e registo de comunicações de natureza semelhante – que, sendo dados informáticos em si mesmos, se apresentam como qualitativamente diversos, em função do nível de intromissão na vida privada e nas comunicações que a sua apreensão é suscetível de importar.

Ora, como se disse, o artigo 17º da Lei do Cibercrime remete para o regime da apreensão de correspondência previsto no Código de Processo Penal (no já citado artigo 179º).

Como sintetizou o acórdão deste Tribunal da Relação de Lisboa de 05.05.2022 [\[5\]](#), “A remissão efetuada pelo art.º 17.º para o regime da correspondência, abrange quatro pressupostos específicos daquele regime:

- i. a referência à nulidade;
- ii. ao facto de ser aplicável a correio eletrónico e registos de comunicação de natureza semelhante enviado ou recebido pelo suspeito, mesmo que de um endereço eletrónico de outra pessoa;
- iii. a proibição de apreensão de correio eletrónico e registos de comunicação de natureza semelhante trocado entre arguido e o seu defensor; e
- iv. O facto de ter que ser o juiz que autorizou ou ordenou a diligência o primeiro a tomar conhecimento do respetivo teor.

O legislador criou um regime específico para apreensão de correio eletrónico e registos de comunicação de natureza semelhante, o que faz com que a respetiva apreensão não seja abrangida na previsão normativa do art.º 16.º, da Lei do Cibercrime.

(...)

Sobre esta questão escreveu Sónia Fidalgo (*A apreensão de correio eletrónico e a utilização noutra processo das mensagens apreendidas*, in Revista Portuguesa de Ciência Criminal, Ano 29, Janeiro-Abril de 2019, p. 73.) dizendo que o art.º 17.º, da Lei do Cibercrime, para além de expressamente fazer uma remissão para o regime de apreensão de correspondência previsto no Código de Processo Penal (art.º 179.º, n.º 1), o próprio art.º 17.º, daquela Lei determina que “*quando, forem encontrados, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova*”; a lei exige claramente um despacho judicial prévio a qualquer apreensão.

Enquanto se mantiver a redação atual, não deve o Ministério Público na sua função de direção do inquérito obedecendo em todas as intervenções processuais a critérios de estrita objetividade, deixar de requerer autorização judicial para a apreensão de correio eletrónico.”

Esta foi, também, a reflexão do Tribunal Constitucional, no referido acórdão nº 678/2021, ao considerar que “A avaliação da conformidade constitucional das normas questionadas exige, porém, um juízo que vá além da mera verificação da *possibilidade abstrata* de restrições aos direitos fundamentais em causa em sede de processo penal, exigindo a análise atenta do cumprimento das exigências constitucionais de excepcionalidade, determinabilidade *proporcionalidade*, bem como das demais regras e princípios constitucionais aplicáveis. Este exercício pressupõe a consideração das concretas condições de aplicação, definidas pelas normas objeto de fiscalização, tal como acima se descreveram.

Nestes termos, cabe assinalar que, como se referiu, a alteração introduzida ao regime jurídico de apreensão do correio eletrónico ou similar, resultante das normas questionadas, que se afigura mais desafiante, do ponto de vista jurídico-constitucional é a atribuição ao Ministério Público, em sede de inquérito, e na qualidade de *autoridade judiciária competente*, para autorizar ou ordenar a apreensão.

Efetivamente, resulta das disposições combinadas dos artigos 263.º, n.º 1, e 1.º, alínea b), do Código de Processo Penal, que o Ministério Público será, em regra, a *autoridade judiciária competente* para a prática de atos no inquérito, na medida em que lhe incumbe a direção desta fase processual. O mesmo não sucede nas restantes fases, designadamente, na instrução, cuja direção cabe, nos termos do artigo 288.º, n.º 1, do CPP, a um juiz.

Ora, Ministério Público e juiz (no caso, o Juiz de Instrução Criminal) têm, à luz da Constituição e da lei, natureza e funções substancialmente distintas. Ao

primeiro compete, segundo o n.º 1 do artigo 219.º da CRP e o artigo 2.º do Estatuto do Ministério Público (doravante, “EMP”, aprovado pela Lei n.º 68/2019, de 27 de agosto), representar o Estado e defender os interesses que a lei determinar, participar na execução da política criminal definida pelos órgãos de soberania, exercer a ação penal orientada pelo princípio da legalidade e defender a legalidade democrática.

A CRP prevê ainda que o Ministério Público goze de um *estatuto próprio* e de *autonomia* (artigo 219.º, n.º 2), o que pressupõe a sua vinculação a critérios de legalidade e objetividade e pela exclusiva sujeição dos magistrados do Ministério Público às obrigações decorrentes do respetivo Estatuto (artigo 3.º do EMP), e não aos demais órgãos do poder público. Contudo, a Constituição concebe o Ministério Público como uma magistratura *responsável e hierarquicamente subordinada* (artigo 219.º, n.º 4 da CRP e artigo 14.º do EMP), sujeita a ação disciplinar por parte da Procuradoria-Geral da República (artigo 219.º, n.º 5 da CRP).

Quanto aos juizes, são *titulares de órgãos de soberania*, com competência para *administrar a justiça em nome do povo*, assegurando *a defesa dos direitos e interesses legalmente protegidos dos cidadãos*, reprimindo a violação da legalidade democrática e dirimindo os conflitos de interesses públicos e privados (artigo 202.º, n.ºs 1 e 2 da CRP e artigos 1.º e 3.º do Estatuto dos Magistrados Judiciais – doravante “EMJ”, constante da Lei n.º 21/85, de 30 de julho, com as alterações decorrentes, por último, da Lei n.º 2/2020, de 31 de março).

Os juizes desempenham as suas funções em condições de estrita *independência* (artigo 203.º da CRP), não estando sujeitos a quaisquer ordens ou instruções (artigo 4.º do EMJ), gozando das garantias de *irresponsabilidade, inamovibilidade*, e outras previstas na lei (artigos 4.º a 6.º do EMJ), e vinculados a exigências de atuação *imparcial, isenta e de respeito pelo princípio da igualdade* (nos termos do disposto nos artigos 6.º-B e 6.º-C do EMJ).

No plano específico do processo penal, o artigo 32.º, n.º 4, da CRP assegura que toda a instrução é da competência de um juiz, não podendo este delegar noutras entidades a prática dos atos instrutórios que se prendam diretamente com os direitos fundamentais. (42)

De tudo o que acaba de expor-se, resulta um retrato distinto da natureza, funções, e garantias associadas à intervenção processual do juiz e do Ministério Público, bastante relevante para a presente análise.

É certo que, como já vimos, a Lei Fundamental permite expressamente *a ingerência das autoridades públicas* na comunicação, nas suas várias formas, nos casos *previstos na lei*, em sede de *processo penal*. Além disso, não resulta

diretamente da norma do n.º 4 do artigo 34.º da CRP que tal ingerência deva ocorrer, necessariamente, mediante intervenção de uma autoridade judicial. A este propósito, disse-se no Acórdão n.º 4/2006:

«O artigo 34.º da CRP, após proclamar, no n.º 1, a inviolabilidade do domicílio e do sigilo da correspondência e dos outros meios de comunicação privada, considera, no n.º 4, “*proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os demais casos previstos na lei em matéria de processo criminal*” (o inciso “*e nos demais meios de comunicação*” foi aditado pela revisão constitucional de 1997, tendo em vista as modernas formas de comunicação à distância, que não correspondem aos sentidos tradicionais de correspondência ou de telecomunicações). Da formulação literal do n.º 4 do artigo 34.º da CRP resulta a limitação direta da admissibilidade da “ingerência ... nas comunicações” ao âmbito do *processo criminal* e a sua sujeição a *reserva de lei*. Mas desse preceito constitucional já não resulta, ao menos de forma explícita e direta, a sujeição da “ingerência” a *reserva de decisão judicial*, como, diversamente, o precedente n.º 2 faz relativamente à entrada no domicílio dos cidadãos contra a sua vontade, que só pode ser ordenada “*pela autoridade judicial competente, nos casos e segundo as formas previstas na lei*” .»

Neste prisma, poderia defender-se que a intervenção do Ministério Público, enquanto *autoridade judiciária competente*, na fase de inquérito, bastaria – atenta a sua *autonomia* e os estritos critérios de *legalidade* pelos quais deve pautar-se a sua intervenção processual – para assegurar a conformidade constitucional da solução legal prevista nas normas questionadas. Sucede, porém, que, tratando-se, como se demonstrou, de *normas restritivas* de direitos, liberdades e garantias, a afetação de tais direitos deverá ser a *menor possível*, devendo limitar-se ao mínimo indispensável para assegurar uma efetiva prossecução dos bens e valores jusconstitucionais que fundamentam a restrição. Ora, considerando o impressionante e distinto retrato do juiz e do Ministério Público que resulta do texto constitucional e das disposições legais aplicáveis – vistos os seus diferentes estatutos e poderes – parece incontornável reconhecer que a *intervenção judicial* constitui uma *garantia adicional de ponderação* dos direitos e liberdades atingidos no decurso da investigação criminal (veja-se o que se disse nos Acórdãos n.º^S 42/2007, n.º 155/2007, n.º 228/2007 e n.º 213/2008).

Efetivamente, nos momentos processuais em que esteja em causa uma *atuação restritiva* das autoridades públicas no âmbito dos direitos fundamentais, a intervenção de um juiz – com as virtudes de *independência* e

imparcialidade que tipicamente a caracterizam - é essencial para uma tutela efetiva desses direitos, mesmo nos casos em que estes devam parcialmente ceder, em nome da salvaguarda de outros bens jusconstitucionalmente consagrados. O juiz tem, nos termos da CRP, uma *competência exclusiva e não delegável* de garantia de direitos fundamentais no âmbito do processo criminal (à luz do artigo 32.º, n.º 4, do CPP), pelo que a lei apenas pode dispensar a sua intervenção em casos excepcionais devidamente delimitados e justificados. Por outras palavras, tal dispensa é constitucionalmente admissível apenas em situações pontuais e definidas com rigor, em que não constitua um *meio excessivo* para prosseguir interesses particularmente relevantes de investigação criminal. Será o caso, por exemplo, de atuações preventivas ou cautelares, em que haja particular urgência ou perigo na demora no que toca à conservação de elementos probatórios, e desde que se assegure uma posterior validação judicial da atuação das autoridades competentes. (43)” Ora, precisamente, com o presente recurso pretende o Ministério Público que se reconheça que tem competência para, *sem prévia autorização judicial* (nos termos do artigo 179º, nº 1 do Código de Processo Penal), ordenar a apreensão de ficheiros de correspondência eletrónica, sem visualização destes pelo OPC ou pelo próprio Ministério Público (após o que os ditos ficheiros de correspondência eletrónica seriam apresentados, intactos, ao Juiz de Instrução Criminal para tomar conhecimento do seu conteúdo e, caso os entenda relevantes, ordenar a junção).

E esta é a perspetiva em que deve ser encarada a pretensão formulada pelo Ministério Público perante este Tribunal: sustentar que, por via da determinação do titular do inquérito, não se procedeu à apreensão de «correspondência eletrónica», mas sim à apreensão de «dados eletrónicos», é, na verdade, um jogo de palavras - posto que, como já vimos, o correio eletrónico não deixa de compor-se de «dados eletrónicos» especialmente protegidos^[6]. Neste âmbito, o ponto que merece destaque - por resultar evidente da factualidade documentada nos autos - é que o Ministério Público, previamente à realização da busca levada a cabo nos escritórios da “T..., Ldª”, estava ciente de que ali seriam encontrados ficheiros de correio eletrónico, tanto assim que solicitou previamente ao Juiz de Instrução Criminal autorização para que se procedesse à respetiva apreensão.

É certo que o Juiz de Instrução *a quo* não chegou a pronunciar-se sobre tal solicitação - mas desse silêncio, mesmo que se considere suscetível de configurar omissão de pronúncia, não pode extrair-se qualquer argumento suscetível de validar a apreensão determinada pelo Ministério Público. Cabi-lhe, na verdade, ter insistido pela decisão omitida, com recurso aos mecanismos legais à sua disposição, o que não fez.

No quadro descrito não pode, pois, considerar-se que o Ministério Público – ou o OPC que levou a cabo a busca não domiciliária por este ordenada – tenha sido *surpreendido* pela existência de ficheiros de correio eletrónico nos computadores da entidade buscada.

Sublinha-se, mais uma vez com o acórdão TC nº 687/2021, que “numa matéria com um grau significativo de *indeterminabilidade* – especialmente problemática por nos encontrarmos em sede de processo criminal –, e atenta a dificuldade de determinação, no plano prático, do significado concreto de conceitos como “mensagens de natureza semelhante ao correio eletrónico”, num contexto de permanente evolução tecnológica, a intervenção prévia à respetiva apreensão de um Juiz de Instrução Criminal afigura-se como essencial para tutela dos direitos, liberdades e garantias afetados. (44)

Nestes termos, considerando todos os argumentos até agora aduzidos, não se duvida de que os interesses prosseguidos pela investigação criminal constituem razões legítimas para uma afetação restritiva dos direitos fundamentais à inviolabilidade da correspondência e sigilo das comunicações (artigo 34.º, n.ºs 1 e 4, da CRP), e à proteção dos dados pessoais, no domínio da utilização da informática (artigo 35.º, n.ºs 1 e 4 da Lei Fundamental), enquanto manifestações particular e intensamente tuteladas da *reserva de intimidade da vida privada* (n.º 1 do artigo 26.º da CRP). Contudo, a restrição de tais direitos especiais, que correspondem a refrações particularmente intensas e valiosas de um direito, mais geral, à privacidade, não pode deixar de respeitar não apenas as condições genericamente impostas pelo texto constitucional para qualquer lei restritiva de direitos fundamentais, nos termos do artigo 18.º, n.º 2, da CRP, como a exigência específica, em sede de processo criminal, de intervenção de um juiz, consagrada no artigo 32.º, n.º 4, da Constituição.

Na verdade, como se procurou explicar, a Lei Fundamental reconhece tal relevo aos interesses e aos valores que a investigação criminal visa salvaguardar que expressamente permite a restrição, quando o não faz noutros âmbitos. Todavia, também não se olvida que o potencial ablativo da liberdade dos cidadãos é particularmente elevado em sede de processo penal, pelo que a CRP impõe a *intervenção do Juiz de Instrução Criminal*, enquanto titular de órgão de soberania independente, imparcial, e especialmente vocacionado para a proteção dos direitos fundamentais, sempre que se revele necessário garantir que os direitos e liberdades dos cidadãos não sofrem compressões desadequadas, desnecessárias ou desproporcionais, e para prevenir que intervenções restritivas abusivas atinjam a sua esfera jusfundamental. Existe, pois, uma ligação muito estreita entre a autorização constitucional de restrição, prevista no n.º 4 do artigo 34.º da CRP, e a

previsão de competência primária do Juiz de Instrução Criminal para a prática de atos que diretamente contendam com direitos fundamentais, estatuída no n.º 4 do artigo 32.º da Constituição. Por isso, e como se disse, uma solução legal que dispense a prévia autorização daquele para a prática de atos de investigação penal que importam a invasão da esfera privada dos cidadãos só será constitucionalmente legítima se existir uma justificação cabal, robusta e bem determinada, não podendo, em caso algum, exceder os limites apertados de uma *solução* excepcional. (45)”

E, com esta conclusão, alcançamos o ponto fundamental da discussão em curso nos autos: estando o Ministério Público ciente, ao determinar a realização da busca não domiciliária, de que a mesma teria como consequência a interferência em dados protegidos – nomeadamente, comunicações de correio eletrónico – não pode acolher-se àquela que se configura como *válvula de segurança* do sistema, a mencionada situação *excecional* tida em vista no artigo 16º da Lei do Cibercrime. Aceitar tal asserção seria sufragar, precisamente, a posição que o acórdão TC 678/2021 julgou inconstitucional.

Cabe, pois, concluir que a pesquisa de mensagens de correio eletrónico tem que ser autorizada *previamente* pelo Juiz de Instrução, nos termos dos artigos 179º e 269º, nº 1, alínea *d*) do Código de Processo Penal e artigo 17º da Lei do Cibercrime^[7], o que não sucedeu no caso em apreço.

A consequência dessa omissão não pode deixar de ser a nulidade da apreensão – que corresponde, na verdade, a uma proibição de prova – como decorre do disposto no artigo 179º do Código de Processo Penal.

Assim, nenhum reparo merece o despacho recorrido.

*

Decisão

Nos termos e pelos fundamentos expostos, acordam os Juízes da 5ª secção do Tribunal da Relação de Lisboa em negar provimento ao recurso interposto pelo Ministério Público, mantendo o despacho recorrido nos seus precisos termos.

Sem custas.

Notifique.

*

Lisboa, 25 de outubro de 2022

(texto processado e integralmente revisto pela relatora – artigo 94º, nº 2 do Código de Processo Penal)

Sandra Oliveira Pinto

Mafalda Sequinho dos Santos

Capitolina Fernandes Rosa

[1] De 30.08.2021, Relatora: Conselheira Mariana Canotilho, acessível em www.tribunalconstitucional.pt, o qual teve por objeto a fiscalização preventiva da constitucionalidade das alterações propostas para o artigo 17º da Lei do Cibercrime constantes do Decreto nº 167/XIV, aprovado pela Assembleia da República em 20 de julho de 2021, tendo-se concluído pela desconformidade constitucional das mencionadas alterações, por violação das normas constantes dos artigos 26º, nº 1, 34º, nº 1, 35º, nº 1 e 4, 32º, nº 4, e 18º, nº 2 da Constituição da República Portuguesa, cuja jurisprudência é particularmente relevante para a questão que temos em mãos, atendendo a que o Tribunal Constitucional procedeu a uma análise detalhada do regime vigente, em contraponto com as alterações aprovadas pela Assembleia da República.

[2] Publicada no Diário da República, Iª série, Nº 179, de 15 de setembro de 2009.

[3] Carta dos Direitos Fundamentais da União Europeia (2016/C 202/02), JO 07.06.2016 - consultável em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR> - merecendo destaque, neste âmbito, os respetivos artigos 7º e 8º, que consagram o respeito pela vida privada e familiar e a proteção de dados pessoais, respetivamente, bem como o artigo 52º, relativo ao âmbito e interpretação dos princípios.

[4] <https://curia.europa.eu/juris/document/document.jsf?jsessionid=B253AE3E8B6C098CCD0B8263FD1F057E?text=&docid=238381&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&>

[5] No processo nº 305/19.7T9AGH-A.L1-9, Relatora: Desembargadora Maria José Cortes Caçador, acessível em www.dgsi.pt, aí se mencionando, também, que sobre esta temática se pronunciaram, designadamente, os acórdãos do Tribunal da Relação do Porto de 09.12.12, do Tribunal da Relação de Lisboa de 01.11.2011, de 07.03.2018, de 0.02.2021 e de 22.02.2022, e do Tribunal da Relação de Évora de 20.01.2015, entre muitos outros, nos quais se entende ser exigível a intervenção judicial.

[6] Como, incisivamente, se fez notar na declaração de voto aposta no Acórdão nº 678/2021, já citado, pelos Conselheiros J.A. Teles Pereira e Maria José Rangel de Mesquita, “a proteção do sigilo das comunicações eletrónicas abrange, como não poderia deixar de ser, tanto os dados circunstanciais de comunicações pretéritas (os *dados de base, localização e tráfego, rectius, metadados*) como o próprio conteúdo dessas comunicações (os *dados de*

conteúdo). E, com efeito, como se diz no presente aresto, nenhum respaldo obtém na jurisprudência constitucional qualquer afirmação contrária a esta, sendo evidente que o conteúdo das próprias comunicações sempre representará um *plus* muito significativo de ofensividade, efetiva ou potencial, ao direito à incolumidade das telecomunicações e à privacidade colocada em causa pela intervenção nestas. Isso mesmo, aliás, obtém claro respaldo na jurisprudência do TJUE, desde o Acórdão *Digital Rights Ireland* (de 8/4/2014, C-293/12 e C-594/12, ECLI:EU:C:2014:238), circunstância que no contexto que ora nos interpela (em que estão em causa *dados de conteúdo*) deve ser destacada. Com efeito, em *Digital Rights* não deixou o Tribunal de Justiça de afirmar que o acesso ao *conteúdo das comunicações eletrónicas*, contrariamente ao que sucede com o acesso aos dados circunstanciais dessas comunicações, afeta o *conteúdo essencial do direito fundamental ao respeito da vida privada* (ponto 39 do Acórdão).”

[7] No mesmo sentido, vd., os acórdãos deste Tribunal da Relação de Lisboa de 22.02.2022 (processo nº 8811/17.1T9SNT-A.L1-5, Relatora: Desembargadora Alda Tomé Casimiro) e de 30.09.2021 (processo nº 3546/20.0JFLSB-A.L1-9, Relatora: Desembargadora Lúcia Trovão), ambos disponíveis em www.dgsi.pt.